REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
17-05-2005	FINAL	

4. TITLE AND SUBTITLE Space Dependence – A Critical Vulnerability of the Net-Centric Operational Commander

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Lt Col Matthew E. Grant

Paper Advisor (if Any): Prof. William Martel

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted to the faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

The U.S. military of today is increasingly dependent on highly integrated, complex C2 systems at all levels of command. These complexities have the potential to cause a break down of C2 required by the operational commander. C2 failures become possible if supportive satellite systems are compromised by threats of natural means, rogue states, or non-state actors. Military commanders and systems dependent on satellite information, data and processes must have alternative systems available to mitigate the loss of satellites at risk and vulnerable to attack. Today the U.S. military utilizes commercial satellites, which are typically not shielded or hardened for both kinetic and non-kinetic threats. Therefore, satellite protection is imperative in the 21st century. With a near-peer competitor like China or the potential instability and aggression of North Korea, the U.S. must consider all possibilities in defense of our national interests. Operational commanders should promote and support the development of innovative techniques and procedures, to negate such threats to command and control networks and associated systems that are critical to combatant forces and their victory in war.

15. SUBJECT TERMS
Satellite vulnerabilities, GPS, EMP, ASAT, anti-satellite, orbits, kinetic weapons, non-kinetic weapons, C2.

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Chairman, JMO Dept
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED		22	**19b. TELEPHONE NUMBER** *(include area code)* 401-841-3556

Standard Form 298 (Rev. 8-98)

NAVAL WAR COLLEGE
Newport, RI

Space Dependence - A Critical Vulnerability of the Net-Centric Operational Commander

By

Matthew E. Grant
Lt Col ANG

A paper submitted to the faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: _____

17 May 2005

Abstract

The U.S. military of today is increasingly dependent on highly integrated, complex C2 systems at all levels of command. These complexities have the potential to cause a break down of C2 required by the operational commander. C2 failures become possible if supportive satellite systems are compromised by threats of natural means, rogue states, or non-state actors. Military commanders and systems dependent on satellite information, data, and processes must have alternative systems available to mitigate the loss of satellites at risk and vulnerable to attack. Today the U.S. military utilizes commercial satellites that are typically not shielded or hardened both kinetic and non-kinetic threats. Therefore, satellite protection is imperative in the 21st century. With a near-peer competitor like China or the potential instability and aggression of North Korea, the U.S. must consider all possibilities in defense of our national interests. The cascading effects of C2 degradation could be attributed to space systems and their vulnerabilities to natural and enemy threats. Operational commanders should promote and support the development of innovative techniques and procedures, to negate such threats to command and control networks and associated systems that are critical to combatant forces and their victory in war.

Table of Contents

Introduction

When a conflict erupts in space, the consequences could have far-reaching affects given how space is essential to globalization of our interdependent world. The myriad of systems in space today provide persistent and real time communications, information, and connectivity to all parts of the world; what better way to connect world economies and societies but through the heavens above. Considering these enormous capabilities, the twenty first century has found space as the only sanctuary from the fog and ravage of war; it is the only theater void of destruction from the fire and steel found in combat. The second 9/11 is conceivably on a distant horizon and given its inherent vulnerabilities, space very well might be the next fertile medium for such an act.

The United States' ever-increasing dependence on satellite information, data, and processes is a "known known"[1] by both U.S. allies and enemies. Space superiority is therefore imperative for U.S. national security. Control and protection of U.S. military and commercial space assets are critical responsibilities in this era of non-state radical fundamentalists and potential belligerent state actors. Space is therefore a plausible frontier for terrorist acts and aggression; such acts would likely have far-reaching and devastating affects on the U.S. and world. If life has little to no value to the enemy, then the destruction of the networked infrastructure of our globalized, interdependent world is a ripe target and a probable part of their grand strategy of terror. The western view of implausible acts changed with 9/11, thus the attack of vulnerable space assets should be planned for, and preemptively countered, through all available means -- diplomatic, informational, military and economic. Nuclear weapon wielding rogue states or radical extremists could destroy or severely degrade the U.S. electrical systems and infrastructure with the electro-magnetic pulse (EMP) of a

[1] Donald H. Rumsfeld, Department of Defense news briefing, 12 February 2002.

nuclear detonation in low earth orbit over central United States.[2] Space is also a theater susceptible to covert destructive actions by peer competitors or adversaries, with the intent and resources to degrade U.S. space capabilities.

Military commanders and systems dependent on satellite information, data and processes must have alternative means of communication and data transfer to mitigate the loss of satellites at risk and vulnerable to attack. The mitigation of such risk must be integral to command and control (C2) networks and hardware designs of satellites and their dependent systems; as well as embedded in flexible and innovative military cultures and doctrine, to ensure heightened protection and security of space-based assets. In the U.S. military push for transformation, Net-Centric Warfare (NCW), and the integration of computer and network based systems become ever more complex and interdependent. The safeguarding of U.S. space resources is required to remain in step with this transformation or net-centricity that is becoming more integral to the U.S. military. This foundation could become a critical weakness instead of a strength to be exploited. The underlying argument of the paper is that the operational commander must understand the importance of identifying the utility and vulnerabilities of the highly space dependent systems available to the warfighter.

Transformation has been apparent in recent history and the evolution of U.S. military actions. The Deputy for Military Space, Office of the Undersecretary of the Air Force, Major General Robert Dickman, USAF (ret), illustrated the evolution of U.S. space dependence. "We had very few weapon systems then [during Desert Storm] that could not have been .ued without space assets. It was very different in Operation IRAQI

[2] William Graham. *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack,* Volume 1: Executive Report, 2004. <http://www.globalsecurity.org/wmd/library/congress/2004_r/04-07-22emp.pdf> [5 Apr 2005].

FREEDOM. The way we planned our campaign-things like GPS were not a force enhancement but embedded in how we operate our forces. And that was a very fundamental difference."[3] In effect, the U.S. moved from satellite-supported military capabilities to full satellite integration, inherent and essential to military operations.

Analysis

In July 2002, the Office of Homeland Security published the National Strategy for Homeland Security. Some objectives of this publication are "Protecting Critical Infrastructures and Key Assets…Threat and Vulnerability….Defending against Catastrophic Threats." The security of U.S. national airspace is specifically identified in the publication but space above the homeland is never mentioned. Although not a Transportation Security Administration responsibility, "defending against catastrophic threats"[4] in or from space must be addressed and understood at every level of government, especially Homeland Security. This is important not only to the military, but also to the federal agencies that are responsible for maintaining stability and security of domestic infrastructures-whether utilities, economic, communications, or transportation. To make a case for these concerns, one must evaluate potential enemy capabilities. Today, over twenty countries have developed missile launch capabilities, which could realistically place a weapon in low earth orbit.[5]

Seven years ago a U.S. satellite, the Galaxy IV, experienced temporary failure of certain functions and for two weeks, over eighty percent of U.S. pagers and other media

[3] J. R. Wilson, "The Ultimate High Ground," *Armed Forces Journal*, January 2004, 28.
[4] Office of Homeland Security, *National Strategy for Homeland Security*, July 2002, 7, 29, 37.
[5] Joint Technical Coordinating Group on Aircraft Survivability (JTCG/AS), *Aircraft Survivability, Surviving Space, Ensuring Aerospace Systems Survivability in the Final Frontier*, Winter 2000, 8. <http://jtcg.jcte.jcs.mil:6101> [14 Apr 2005].

signals were out of service.[6] Although this was an internal problem of the satellite, one can only imagine if aggressive intent and capability were the root cause in such a situation. The two weeks could have become months or longer. Unintentional malfunctions, in and of themselves, can cause significant problems in highly interdependent systems and processes, as in the following examples. In 2001, California experienced interruptions of their electric power supplies, in which a non-deliberate degradation of such a fundamental need had far-reaching consequences that stymied their normally robust agriculture and oil industries.[7] The worldwide free flow of unbiased and factual information through satellite relayed media sources is not without censorship. In July 2003, Arabic television broadcasts from a U.S. satellite (Telestar-12) were jammed. Iranian journalists working with the Voice of America developed uncensored news programs for the Iranian people. Although satellite TV receivers are forbidden in Iran, more than one million Iranians are connected to the real world but are not without risk. Because of the unrest, such broadcasts could insight; the Iranian government working with Cuba was able to jam the Telstar-12 using equipment designed for communications intelligence gathering.[8] If Cuban anti-satellite (ASAT) jamming capabilities are such that U.S. media relays and broadcasts can be degraded or denied, one can only imagine the jamming capabilities states such as North Korea, China, and Russia might possess.

Electro Magnetic-Pulse (EMP) and other non-kinetic threats are as potentially damaging as kinetic threats. Kinetic threats, both natural and manufactured, are highly

---

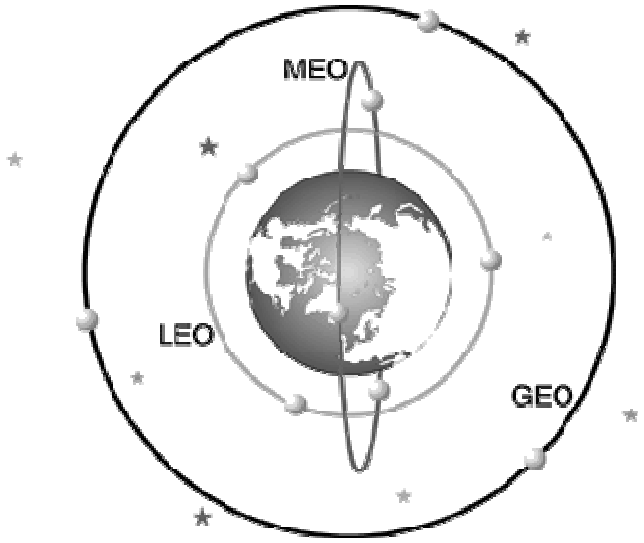
[6] Office of the Secretary of Defense, *Report of the Commission to Assess United States National Security Space Management and Organization*, Executive Summary, 11 Jan 2001, 14.
[7] Manuel Cereijo. *Dangerous Threat: Infrastructure Interdependencies*, n.d. <http://www.amigospais-guaracabuya.org/oagmc188.php> [10 Apr 2005].
[8] Michael Waller., "Homeland Insecurity, Iran, Cuba Zap US Satellites, Official Likens Communications Jamming to 'Act of War'," *WorldNet Daily*, 7 Aug 2003. <http://www.wnd.com/news/article.asp?ARTICLE_ID=33957> [10 Apr 2005].

affected by the factors of space and time. Although satellite positions are known, the interception of a satellite in an orbit hundreds or thousands of miles above the earth will be much more challenging than the omni-directional propagation of thermal radiation from a nuclear detonation. EMP is the result of a gamma radiation reaction with molecules in the earth's atmosphere. This reaction spreads at the speed of light from the nuclear explosion, disrupting or destroying any electromagnetic device or signal in the earth's atmosphere and the blast's path.[9] The effectiveness of the weapon depends on the altitude and yield of the detonation. In such a devastating display of terrorism, the result could potentially disrupt or destroy the functions of navigation systems, communications, environmental data, missile warning, surveillance and reconnaissance, and space control systems. If the active satellites are not kinetically or electromagnetically affected because of extreme distances or orbit patterns during an EMP event, the uplink and downlink transmissions are subject to degradation or denial.

EMP is normally associated with a nuclear detonation, but today and tomorrow's weapon technologies will enable a belligerent to disrupt or destroy the circuitry of unshielded or non-hardened electronic devices without a nuclear yield. Non-nuclear EMP devices have been developed and are inexpensive in comparison to nuclear weapons, yet without the constraints associated with nuclear material.[10] It is conceivable for an EMP weapon to be deployed into a theater of war using a ship or ground launched missile. The well-known Patriot Air Defense system used in DESERT STORM is very capable against missiles and

9 Air University, *Space Primer*, August 2003, 22-2. <http://space.au.af.mil/primer/> [13 Apr 2005].
10 MILNET, *E-Bomb - Electro Magnetic Pulse Weapon*, 2002. <http://www.milnet.com/e-bomb.htm> [2 Apr 2005].

aircraft; however, every surface-to-air missile system has range and altitude limitations.[11] Without the threat of anti-ballistic missile systems, a ground or ship launched EMP laden missile would likely find success on the battlefield. EMP weapon employment would be most effective at altitude. Given enough distance from any capable defensive systems, EMP would propagate commensurate with its strength and position causing disruption or destruction of electronic devices critical to weapons employment, command, control, communications and information processing.[12]



LEO – Low Earth Orbit (100-500 miles) - Satellite phone, Military, Observation
MEO – Medium Earth Orbit (6,000-12,000 miles) - Weather Satellites, Observation
GEO – Geostationary Earth Orbit (≈22,300 miles) - Television, Communications

Figure 1. Orbit Classification with Satellite Types[13]

China, with its vibrant economic growth and a massive workforce has become a near-peer competitor of the U.S. With this rise to power, its space program is acquiring abilities,

11 Army-Technology.com, *Patriot Missile Air Defense System*, n.d. <http://www.army-technology.com/projects/patriot/> [10 May 2005].
12 MILNET, *E-Bomb - Electro Magnetic Pulse Weapon*, 2002. <http://www.milnet.com/e-bomb.htm> [2 Apr 2005].
13 InetDaemon.com, *Satellite Orbits*, 4 May 04, <http://www.inetdaemon.com/tutorials/satellite/orbits.html> [20 Apr 2005].

which threaten our advances, and should be feared. As history has shown, power in the wrong hands can sometimes lead to war at the costs of millions of military and civilian lives. Suppose a Nazi-like extremist was to become the next military leader of North Korea or Iran. Could the U.S. counter all the covert and overt aggression by such an opposing state? If this question did not include overt aggression, China surfaces as a candidate. China is an emerging power with competitive spirit, on a quest for legitimacy and respect, both economically and militarily. How better to gain these attributes than to match or exceed the competition in military prowess and economic presence on a global scale. The Chinese economic presence is part of everyday life here in the U.S. as seen by Chinese imports. The total imports to the U.S. for 2005 are estimated at 161.5 billion in comparison to exports totaling 100.5 billion.[14] Chinese economics in the U.S. does not stop with imports, the Washington Times writes, "The possibility of political retaliation on Capitol Hill especially over China's currency manipulation to gain a competitive advantage is growing. The Senate last week overwhelmingly approved an amendment to impose stiff trade sanctions on China unless it stops keeping its currency artificially low."[15]

The FY04 Report to Congress on PRC Military Power brought to light several important aspects of Chinese military potential and intent that must be considered when developing and employing U.S. spaced based systems and processes. The Chinese have maintained the position that space should remain free of offensive military capabilities and therefore are opposed to anti-satellite weapons of any kind. It was also postulated in this report that China believes a militarized space will become a reality. At the time of this

[14] Ron Scherer. "Imports Increasingly Burden US Economy, The Nation's Growth Rate Slowed For The First Quarter - And Oil Prices Aren't The Only Reason," *The Christian Science Monitor*, 29 April 2005, <http://www.christiansciencemonitor.com/2005/0429/p03s01-usec.html> [2 May 2005].
[15] Patrice Hill. "U.S. Flooded by Imports from China," *The Washington Times*, 1 May 2005 <http://washingtontimes.com/business/20050412-093353-9316r.htm> [2 May 2005]

opposition to anti-satellite (ASAT) weapons, they were "developing advanced information technology and long-range precision strike capabilities, and looking for ways to target and exploit the perceived weaknesses of technologically superior adversaries. China is believed to be conducting research and development on a direct-ascent ASAT system that could be fielded in the 2005-2010 timeframe."[16]

Such mentioned emerging capabilities are perhaps warning signs of events to come. Even as the most powerful country in the world, the U.S. might experience a "Space Pearl Harbor"[17] in the future, which could dramatically disrupt U.S. national and global security, causing widespread instability since the globalized economy and the U.S. military are satellite supported and dependent. Such an event in space would cripple the infrastructure in which we depend upon, but routinely take for granted. As a member of the Russian Duma has stated, "You know, if we really wanted to hurt you, we would set off an atomic weapon at high altitude above your country and produce an EMP that would destroy your entire electrical power grid, computer, and telecommunications infrastructure."[18]

The Global Positioning System (GPS) is a collection of satellites in a medium earth orbit (see figure 1), circling the globe once every twelve hours. Global Positioning System supports critical navigation and time functions of both commercial and military systems, and is an essential part of the foundation from which many of these systems are based. In 2004 over three billion dollars was spent on GPS related goods and services, and this figure is

---

[16] Office of the Secretary of Defense, *FY04 Report to Congress on PRC Military Power Pursuant to the FY2000 National Defense Authorization Act,* 28 July 2003, 36-37. <http://www.defenselink.mil/pubs/d20040528PRC.pdf> [6 Apr 2005].

[17] Office of the Secretary of Defense, *Report of the Commission to Assess United States National Security Space Management And Organization,* Pursuant to Public Law 106-65, 11 Jan 2001, 13. <http://www.defenselink.mil/pubs/spaceintro.pdf> [20 Apr 2005]

[18] Air University, *Space Primer,* August 2003, 22-1. <http://space.au.af.mil/primer/> [13 Apr 2005]

expected to increase another seven billion over the next six years.[19] The applications of the Global Positioning System are extensive and should be highlighted, as many are military in nature. For example, Blue Force Tracker (BFT) systems used by the U.S. ground forces have been invaluable to the operational commanders and their combat forces. BFT systems provide detailed battle space situational awareness information and serve as communication links for combat forces and their command elements.[20] In addition, "C2 systems such as the Army Battle Command Systems (ABCS) rely on digitized position reports from all platforms on the battlefield. The predominate source of that position data is the NAVSTAR Global Positioning System (GPS)."[21] This advent of complete or near complete battle space visibility poses a threat to operational commanders, as strategic level decision makers can now, in real-time, circumvent this intermediate level of command; thereby blending operational and tactical levels of war. Command personalities must understand and honor decentralized mission execution in this new age of battle space omni-vision available throughout the ranks of command. Yet another important example of GPS reliance found on the battlefield is with forward air controllers (FACs). Forward air controllers coordinate close air support (CAS) aircraft for enemy suppression. GPS is invaluable to their mission, as they can relay accurate vectors to striking aircraft, thereby minimizing collateral damage and fratricide.[22]

---

[19] Dan Nobbe and Chuck Tabbert,"Space-Based GPS Lowers Satellite Costs," *Electronic Engineering Times*, ProQuest Military Collection, 20 Sept 2004, 51.
[20] Marcorsyscom Magtf C4ISR Ground C2 Systems. *Blue Force Tracker*, 12 May 2005. <http://www.marcorsyscom.usmc.mil/sites/pmgc2/bft.asp> [20 Apr 2005].
[21] Raymond Filler, *Positioning, Navigation and Timing: The Foundation of Command and Control*, US Army Command and Control Directorate (C2D), Fort Monmouth, NJ, n.d., 2. <http://www.dodccrp.org/events/2004/CCRTS_San_Diego/CD/papers/229.pdf> [25 Apr 2005].
[22] 1st Marine Division, "Operation IRAQI FREEDOM (OIF): Lessons Learned," Globalsecurity.com, May 2003 <http://www.globalsecurity.org/military/library/report/2003/1mardiv_oif_lessons_learned.doc> [25 Apr 2005].

There are several arguments for why belligerent aggression will never propagate to space. One plausible argument against is the commercialization and globalization of space makes it an improbable theater of warfare. Considering how multinational corporations and militaries around the world are leveraging the use of space and its capabilities via satellites, the risks are far too great for civilized states and the world economy, if a war was to erupt in space. If threats to satellites and their capabilities are negligible, then the operational commander's C2 systems will remain robust and provide complete battle space awareness. These risks are obvious, but today conflicts can be attributed to fundamentalist extremists. Without the use of a Western mindset for mirror-imaging, the acts that terrorist perpetrate are rational and acceptable in their culture and through their eyes, as their martyrdom in the fight against the western infidels delivers them to Allah. The terrorist attack on 9/11 changed everything and proved that wanton and vile terrorist crimes are possible, especially where they are least expected, as in the case of space.

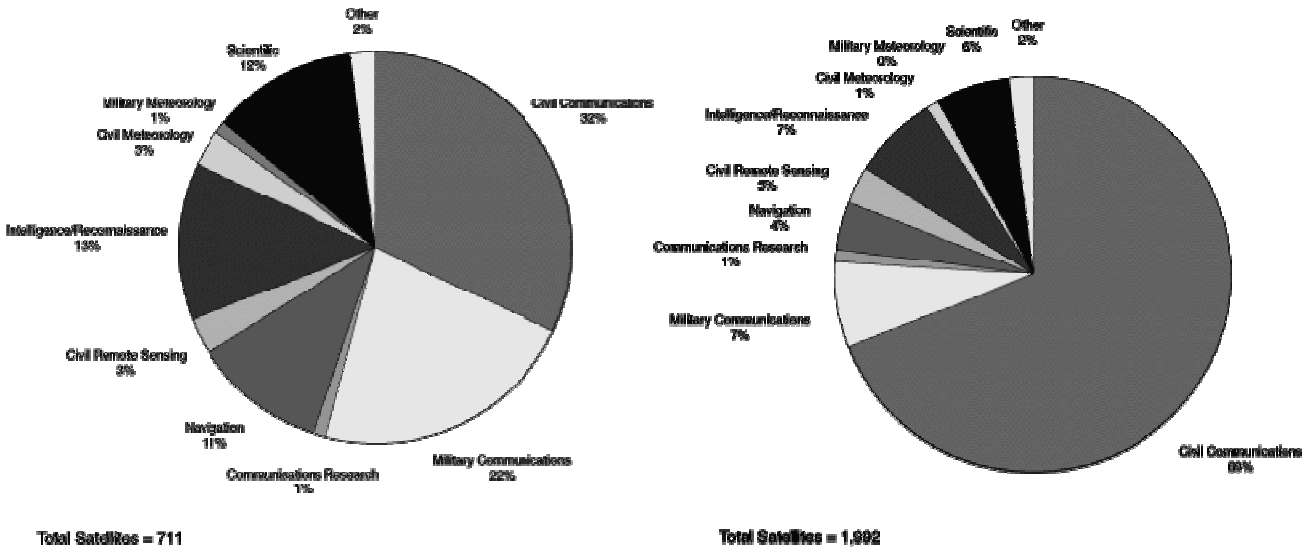
The cost of deploying space-based platforms is on the magnitude of ten thousand dollars per pound. Considering the Department of Defense and the U.S. government's annual budget is under the watchful eye of congress, expenditures of this scale come under close scrutiny in this time of the Global War on Terrorism (GWOT). Currently, the U.S. budget is stressed with the enormous expenditures of war. Therefore, the military and government in general must leverage existing commercial space systems to mitigate to costs of increasing satellite demands. Typically, the U.S. military utilizes more commercial than military satellites, as the ratio in 2010 is expected to be approximately six to one, as shown in figure 2.

Because of the exorbitant costs of satellite deployment and employment, most commercial systems are not shielded or hardened for physical or electromagnetic threat protection. In turn, these satellites are naturally susceptible to damage or degradation from natural occurring threats, as well as common and advanced technologies of belligerent actors. Natural satellite hazards can be kinetic, as in meteorites or particles from the earth's upper atmosphere. These natural hazards also include solar flares and cosmic rays, which are electromagnetic, as are man-made "electromagnetic threats can include lasers, high powered microwaves, and radio frequency (RF) jamming."[23] Although commercial in nature and utilized by multiple clients, these platforms need to be regarded as high value soft targets critical to U.S. national security.

Figure 2 depicts the changes in satellite population and missions over a fourteen-year period, from 1996 to 2010. It is obvious that commercial communications are the satellite growth area and with this shift, the military will increase their dependence on the civilian sector assets thereby creating inherent vulnerabilities.

Along with limited protection as mentioned, satellites maintain very predictable orbits and speeds with very limited maneuver capabilities. These attributes lend to the conditions that an attacker desires in a target. With the endless satellite tracking resources available today, even amateur satellite trackers know the positions and orbits of both U.S. military and commercial satellites. This constitutes a problem in that U.S. enemies know or could know, with minimal effort, where critical satellites are or will be in the future. Without protection and maneuverability while they maintain predictable orbits, satellites in general are inviting to space terrorists or belligerents to act asymmetrically against our capabilities.

[23] Joint Technical Coordinating Group on Aircraft Survivability (JTCG/AS), *Aircraft Survivability, Surviving Space, Ensuring Aerospace Systems Survivability in the Final Frontier*, Winter 2000, 6. <http://jtcg.jcte.jcs.mil:6101> [14 Apr 2005].



1996 **2010**

Figure 2. Satellites by Mission and Year[24]

Recommendations

The U.S. Air Force is aware of and concerned with satellite security and protection, and supposedly has developed capabilities to deny satellite use by known enemies. There are known systems, as well as the plausible but unknown systems, in the U.S. military inventory. "Officially declared operational, meanwhile, was the Counter Communications System (CounterCom), a radio frequency-based system designed to temporarily jam communications satellites, the Air Force said." The realization and concern with this revelation, is the proliferation of anti-satellite capabilities using current commercial electronic technologies that are accessible to potential enemies.[25]

[24] Lt Gen Bruce Carlson, "Protecting Global Utilities Safeguarding the Next Millennium's Space-Based Public Services", *Aerospace Power Journal*, Summer 2000. <http://www.airpower.maxwell.af.mil/airchronicles/apj/apj00/sum00/carlson.htm> [1 Apr 2005].

[25] Jeremy Singer, "Satellite Jammer Ready: U.S. Parallel Effort To Thwart Imaging Craft Dropped," *C4ISRJournal*, 19 October 2004, <http://www.isrjournal.com.story?php?F=461040> [17 Apr2005].

Operational commanders must cultivate organizational cultures that encourage innovative thinking and risk taking, so that techniques and alternatives outside the norm of conventional operations become routine. As described in Space Operations, Air Force Doctrine Document 2-2, commercial satellites were utilized even in the Vietnam War, as they aided in communication of support requirements between Vietnam and the U.S. The Defense Support Program (DSP) played an important missile-warning role during the Cold War and beyond. In "Operation ALLIED FORCE…the DSP constellation achieved new success in Kosovo. Through a "direct support" relationship between a squadron (CONUS) and the CFACC (Italy), real-time information from DSP was fed to the COAC. With this information, coupled with data from unmanned aerial vehicles (UAVs) and imaging satellites commanders were given the BDA information needed to tailor follow-on strike packages."[26] This integrated structure for data flow and processing, minimized human exposure in the battle space and to threats because BDA was achieved with remote controlled sensors.[27] With the introduction of these capabilities, there are increased public influences on U.S. war making policies and practices. In this era of globalization and its worldwide communications networks, the American public has more impact over the battlefield than ever before. Their influence and support is vital to the U.S. strategic center of gravity. Less risk to the human element in war will be accepted or tolerated; therefore, the operational commander must adjust to these changes by leveraging technological capabilities, to remove the human element.

An adversary can use active electronic countermeasures to degrade or deny satellite communications to other satellites, aircraft, and ground systems by over powering or

[26] Department of the Air Force, *Space Operations,* Air Force Doctrine Document 2-2, (Washington DC: 27 Nov 2001), 39.
[27] Ibid.

deceiving the uplinks or downlinks, normally referred to as jamming or electromagnetic interference (EMI) and spoofing. One must take preemptive actions to ensure accurate battle space oversight if GPS is susceptible to jamming; as highlighted in the following statement from a U.S. Army Command and Control Directorate document. "A downside to GPS is its low signal power, making it vulnerable to EMI and signal blockage."[28]

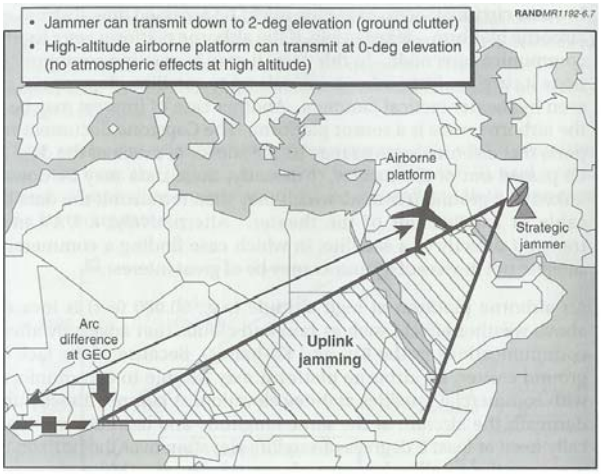


Figure 3. Airborne Platform Using a Low Elevation Satellite to Overcome Strategic Jamming

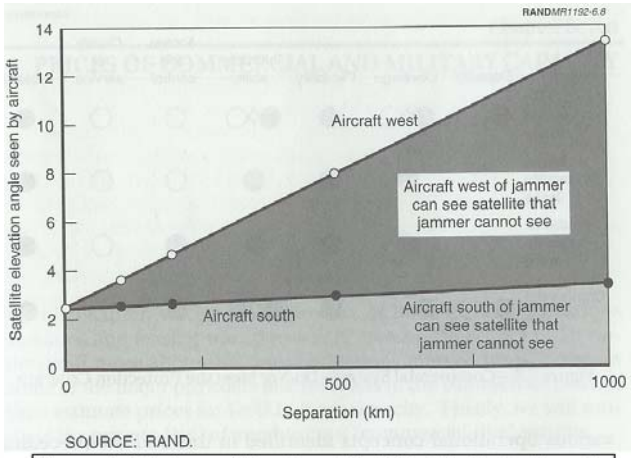


Figure 4. Maximum Elevation of Satellite Visible to Aircraft but Invisible to Ground-Based Jammer [29]

Operational commanders should promote and support the development of innovative techniques and procedures, to negate such threats to command and control networks and associated systems that are critical to the combatant forces. Figures 3 and 4 depict options available to airborne military forces to counter uplink jamming of their satellite assets. Using optimum geometry between the satellite and aircraft positions, the jammer's capabilities can be minimized or negated. The aircraft takes advantage of its altitude to ensure a satellite

[28] Raymond Filler, *Positioning, Navigation and Timing: The Foundation of Command and Control (C2D)* Fort Monmouth, NJ, n.d., 2. <http://www.dodccrp.org/events/2004/CCRTS_San_Diego/CD/papers/229.pdf> [25 Apr 2005].
[29] Tim Bonds, *Employing Commercial Satellite Communications,* Project Air Force, RAND, 2000, 82-83.

uplink, while the ground based jammer becomes ineffective due to its inability to burn through the ground clutter. Although this example touches the tactical realm of combat, the point is that operational commanders need to support creative ideas of their troops. The integral ways and means to ensure connectivity and integration of space-based systems with the battlefield, and ultimately the operational commander, are dynamic and complex. These examples show what is in the drawer of the tool chest, which military tacticians and war planners can provide. A complete description and analysis of techniques, tactics, and procedures is outside the scope of this paper. However, with thorough and continuous assessment and reassessments of their strengths, weaknesses, critical capabilities, and vulnerabilities, the commander can remain in step with the dynamic battle spaces that present themselves.

The U.S. military's evolution towards net-centric warfare systems design, in combination with its ever expanding need for space platforms, has improved C2 capabilities through near complete connectivity throughout the combatant force structure. Unmanned aerial vehicles (UAV) have become more prevalent, as battle space ISR and communication platforms, which in turn can be multi-tasked as secondary or back-ups to satellite resources. Along with UAVs, traditional air breathing assets can also play multiple roles in satellite-out scenarios. A relatively new resource in the vast U.S. military inventory of data collection assets supporting the warfighter are "near space" platforms. These systems are relatively inexpensive to design and develop and their proximity to earth lends to higher image resolution and longer loiter time. Their launch process is simple in comparison to satellites, as these systems are typically large, maneuverable balloons.[30]

30 Alan Boyle, "Airship Groomed for Flight to Edge of Space," *MSNBC,* 21 May 2004 <http://msnbc.msn.com/id/5025388/> [10 May 2005]

One suggestion to consider, illustrated in figure 5, depicts connection options available for different network levels. Of noteworthy importance in figure 5 is the use of cables or hard lines of communication as they are less susceptible to degradation, unless they are severed. The in-theater networks are linked as noted above as well as cellular type

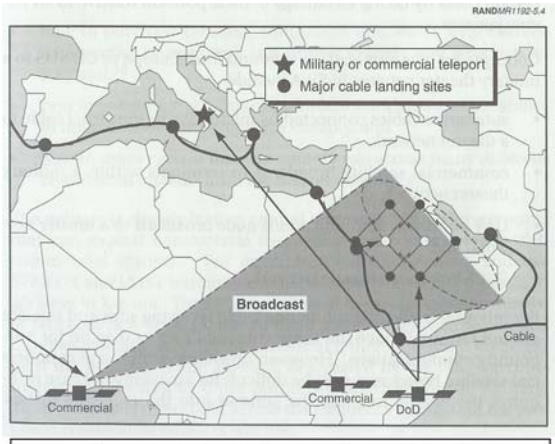


Figure 5. Options to Connect Theater Network to Global Networks[31]

transmissions and space based links.[32] With this combination of links and connections, theater commanders can maintain redundant connectivity with both subordinate and superior commands worldwide.

Conclusion

> Command and control is most effective when decision superiority exists. Decision superiority results from superior information filtered through the commander's experience, knowledge, training, and judgment; the expertise of supporting staffs and other organizations; and the efficiency of associated processes.
>
> Joint Vision 2020[33]

Today the operational commander ultimately makes decisions based on information from sources that are at risk and susceptible to attack. This decision process is highly dependent on current and accurate communications through networks and satellites, both

[31] Tim Bonds, *Employing Commercial Satellite Communications*, Project Air Force, RAND, 2000, 51.
[32] Ibid.
[33] Department of Defense, Joint Chiefs of Staff, *Joint Vision 2020,* (Washington DC: GPO, June 2000), 31.

commercial and military. Central to "decision superiority" is the "efficiency of associated processes."[34] If this efficiency were neutralized, command decisions would consequently be skewed, as information required would be incomplete. Efficiency is based on how effective these information processes interact and are maintained. The cascading effects of this predicament can be attributed to space systems and their vulnerabilities to natural and enemy threats. Given the potential for a 9/11 in space, today's operational commander must be technically astute about critical net-centricity limitations, so in times of incomplete battle space awareness, timely and accurate decisions are made. Measures for security and protection of all space systems must become an integral task of the Department of Defense, as the military systems of tomorrow will not be complete or fully effective without their space components.

[34] Ibid.

Bibliography

1st Marine Division. *Operation IRAQI FREEDOM (OIF): Lessons Learned,* May 2003. <www.gobalsecurity.org/military/library/report/2003/1mardiv_oif_lessons_learned.doc> [25 Apr 2005].

Air Force Doctrine Document (AFDD) 2-2, *Space Operations,* 27 Nov 2001.

Air University, *Space primer,* Maxwell AFB, AL: August 2003. <http://space.au.af.mil/primer/> [13 Apr2005].

Army-Technology.com. *Patriot Missile Air Defense System,* n.d. <http://www.army-technology.com/projects/patriot/> [10 May 2005].

Bonds, Tim. E*mploying Commercial Satellite Communications*, Project Air Force, RAND, 2000.

Boyle, Alan. "Airship groomed for flight to edge of space," *MSNBC,* 21 May 2004 <http://msnbc.msn.com/id/5025388/> [10 May 2005].

Carlson, Bruce Lt Gen. "Protecting Global Utilities Safeguarding the Next Millennium's Space-Based Public Services," *Aerospace Power Journal,* Summer 2000. <http://www.airpower.maxwell.af.mil/airchronicles/apj/apj00/sum00/carlson.htm> [1 Apr 2005].

Caton, Jeffrey. "Joint Warfare and Military Dependence on Space," *Joint Force Quarterly*, Winter 1995-96.

Cereijo, Manuel. *Dangerous Threat: Infrastructure Interdependencies.* n.d. <http://www.amigospais-guaracabuya.org/oagmc188.php> [10 Apr 2005].

Department of Defense, Joint Chiefs of Staff, *Joint Vision 2020,* (Washington DC: GPO, June 2000)

Filler, Raymond. *Positioning, Navigation and Timing: The Foundation of Command and Control,* US Army Command and Control Directorate (C2D), Fort Monmouth, NJ: n.d. <http://www.dodccrp.org/events/2004/CCRTS_San_Diego/CD/papers/229.pdf> [25 Apr 2005].

Graham, William and others. *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack,* Volume 1: Executive Report, 2004 <http://www.globalsecurity.org/wmd/library/congress/2004_r/04-07-22emp.pdf> [5 Apr 2005].

Hill, Patrice. "U.S. Flooded by Imports from China," *The Washington Times,* 1 May 2005. <http://washingtontimes.com/business/20050412-093353-9316r.htm> [5 May 2005].

InetDaemon.com. *Satellite Orbits,* 4 May 04. <http://www.inetdaemon.com/tutorials/satellite/orbits.htm> [2 May 2005].

Joint Technical Coordinating Group on Aircraft Survivability (JTCG/AS), *Aircraft Survivability: Surviving Space, Ensuring Aerospace Systems Survivability in the Final Frontier,* Winter 2000. <http://jtcg.jcte.jcs.mil:6101> [14 Apr 2005].

Marcorsyscom Magtf C4ISR. Ground C2 Systems, *Blue Force Tracker,* 12 May 2005. <http://www.marcorsyscom.usmc.mil/sites/pmgc2/bft.asp> [20 Apr 2000].

Milnet. *E-Bomb - Electro Magnetic Pulse Weapon,* 2002. <http://www.milnet.com/e-bomb.htm> [2 Apr 2005].

Nobbe, Dan; Tabbert, Chuck. "Space-based GPS lowers satellite costs," *Electronic Engineering Times*, ProQuest Military Collection, 20 Sept 2004.

Office of Homeland Security, *National Strategy for Homeland Security,* (Washington DC: July 2002).

Office of the Secretary of Defense, *FY04 Report to Congress on PRC Military Power Pursuant to the FY2000 National Defense Authorization Act,* (Washington DC: 28 July 2003). <http://www.defenselink.mil/pubs/d20040528PRC.pdf> [6 Apr 2005].

Report of the Commission to Assess United States National Security Space Management and Organization, Executive Summary, (Washington DC: 11 January 2001). <http://www.defenselink.mil/pubs/space20010111.html> [20 Apr 2005].

Preston, Bob and others. *Space Weapons – Earth Wars,* RAND, 2002.

Scherer, Ron. "Imports Increasingly Burden US Economy, The Nation's Growth Rate Slowed for the First Quarter - and Oil Prices aren't the only Reason." *The Christian Science Monitor,* 29Apr 2005. <http://www.christiansciencemonitor.com/2005/0429/p03s01-usec.html> [2 May 2005].

Singer, Jeremy. "Satellite Jammer Ready: U.S. Parallel Effort To Thwart Imaging Craft Dropped," *C4ISRJournal*.com, 19 Oct 2004. <http://www.isrjournal.com.story?php?F=461040> [17 Apr 2005].

Waller, Michael. "Homeland Insecurity, Iran, Cuba zap US Satellites, Official likens communications jamming to 'act of war'," *WorldNet Daily,* 7 Aug 2003. <http://www.wnd.com/news/article.asp?ARTICLE_ID=33957> [10 Apr 2005].

Wilson, J. R.. "The Ultimate High Ground," *Armed Forces Journal*, January 2004.